

Husztai Andrea

2016

1. Andrea Husztai, Oláh Norbert  
A simple authentication scheme for clouds  
In: 2016 IEEE Conference on Communications and Network Security (CNS) . Konferencia helye, ideje: Philadelphia , Amerikai Egyesült Államok , 2016.10.17 -2016.10.19. pp. 565-569. (ISBN:978-1-5090-3065-1)  
Befoglaló mű link(ek): [IEEE Xplore](#)  
Egyéb konferenciaközlemény /Konferenciaközlemény /Tudományos

2015

2. Husztai Andrea, Kovács Zita  
Bilinear Pairing-based Hybrid Mixnet with Anonymity Revocation  
In: Olivier Camp , Edgar Weippl , Christophe Bidan , Esma Aïmeur (szerk.)  
ICISSP 2015: Proceedings of the 1st International Conference on Information Systems Security and Privacy . 380 p.  
Konferencia helye, ideje: Angers , Franciaország , 2015.02.09 -2015.02.11. Portugal: SciTePress, 2015. pp. 238-245.  
(ISBN:978-989-758-081-9)

Könyvrészlet /Konferenciaközlemény /Tudományos

3. Husztai Andrea  
Analyzing security requirements for cryptographic protocols  
Benyújtás éve: 2014. Védés éve: 2015.  
Témavezető(k): Pethő Attila.  
2015.  
Disszertáció /Habilitációs anyag /Tudományos

2014

4. Andrea Husztai  
Charles A Shoniregun , Tyson T Brooks (szerk.)  
Anonymous Multi-Vendor Micropayment Scheme based on Bilinear Maps  
In: International Conference on Information Society (i-Society 2014) . Konferencia helye, ideje: London , Egyesült Királyság / Anglia , 2014.11.10 -2014.11.12. IEEE, pp. 27-32.  
Link(ek): [DOI](#)  
Egyéb konferenciaközlemény /Konferenciaközlemény /Tudományos  
Független idéző: 2 Összesen: 2

- 1 *Haiping Huang, Tianhe Gong, Tao Chen, Mingliang Xiong, Xinxing Pan, Ting Dai*  
An Improved  $\mu$ TESLA Protocol Based on Queuing Theory and Benaloh-Leichter SSS in WSNs  
*JOURNAL OF SENSORS* (ISSN: 1687-725X) 2016: pp. 1-13. (2016)  
Folyóiratcikk /Szakcikk /Tudományos
- 2 *Antonio Ruiz-Martínez, Juan A Sánchez-Laguna, Antonio F Skarmeta*  
Extending SIP to support payments in a generic way  
*COMPUTER STANDARDS & INTERFACES* (ISSN: 0920-5489) 46: pp. 23-36. (2016)  
Folyóiratcikk /Szakcikk /Tudományos

2013

5. Andrea Husztai  
Multi-Vendor PayWord with Payment Approval  
In: Kevin Diami , Hamid R Arabnia (szerk.)  
Proceedings of the 2013 International Conference on Security and Management . Las Vegas: CSREA Press, 2013. pp. 265-271.  
(ISBN:1-60132-259-3)

Könyvrészlet /Konferenciaközlemény /Tudományos

Független idéző: 1 Összesen: 1

- 1 *Jia-Ning Lou, Ming-Hour Yang, Yu-Cheng Ho*  
EMV-based mobile payment protocol for offline transaction with the ability of mutual authentication  
*International Journal of Science and Engineering* (ISSN: 2223-4489) 5: (1) pp. 61-66. (2015)  
Folyóiratcikk /Szakcikk /Tudományos

2012

6. László Aszalós , Andrea Husztai  
Payment approval for PayWord  
In: D H Lee , M Yung (szerk.)  
Information Security Applications, LNCS 7690 . Konferencia helye, ideje: Jeju , Dél-Korea , 2012.08.16 -2012.08.18.  
Berlin; Heidelberg: Springer-Verlag, 2012. pp. 161-176.

(ISBN:978-3-642-35415-1)

Link(ek): [DEA](#), [Teljes dokumentum](#)

Könyvrészlet /Könyvfejezet /Tudományos

Független idéző: 2 Összesen: 2

1. *Y Chen, JS Chou*  
Cryptanalysis on "Secure untraceable off-line electronic cash system"  
Cryptology ePrint Archive. (2014.)  
  
Egyéb /Folyóirat vagy sorozatszerkesztés /Tudományos
2. *Y Chen, JS Chou*  
On the Privacy of "User Efficient Recoverable Off-Line E-Cash Scheme with Fast Anonymity Revoking"  
**INTERNATIONAL JOURNAL OF NETWORK SECURITY** (ISSN: 1816-353X) 17: (6) pp. 700-703. (2015)  
Folyóiratcikk /Szakcikk /Tudományos

2011

7. Folláth János , [Husztai Andrea](#) , Pethő Attila  
Informatikai biztonság és kriptográfia: [elektronikus dokumentum]  
Debrecen: Kempelen Farkas Digitális Tankönyvtár, 2011.  
Link(ek): [Teljes dokumentum](#)  
Könyv /Felsőoktatási tankönyv /Oktatási
8. [Husztai A](#)  
A Homomorphic Encryption-Based Secure Electronic Voting Scheme  
**PUBLICACIONES MATHEMATICAE DEBRECEN** 79:(3.-4.) pp. 479-496. (2011)  
*Folyóirat szakterülete: Mathematics (miscellaneous) helyzete: Q3*  
Folyóiratcikk /Szakcikk /Tudományos  
Független idéző: 6 Összesen: 6
  1. *Shubhangi S Shinde, Prof D K Chitre*  
Privacy Preservation in Evoting Using Homomorphic Technology  
**INTERNATIONAL JOURNAL OF LATEST TRENDS IN ENGINEERING AND TECHNOLOGY** (ISSN: 2319-3778) 2: (4) pp. 397-402. (2013)  
Folyóiratcikk
  2. *Shubhangi S Shinde, Sonali Shukla, Prof D K Chitre*  
Secure E-voting Using Homomorphic Technology  
**INTERNATIONAL JOURNAL OF EMERGING TECHNOLOGY AND ADVANCED ENGINEERING** (ISSN: 2250-2459) 3: (8) pp. 203-206. (2013)  
Folyóiratcikk
  3. *M Mesbahuddin Sarker, Dr Md Sharif Uddin*  
Electronic Voting Algorithm and Its Algebraic Formation  
**International Journal of Mathematics Trends and Technology** 10: (1) pp. 26-33. (2014)  
Folyóiratcikk /Szakcikk /Tudományos
  4. *Vamshinath N, Ramya K R, Krishna S, Bhaskar P G, Mwaseba G L, Kim T H*  
Homomorphic Encryption for Cluster in Cloud  
**International Journal of Security and its Applications** 9: (5) pp. 319-324. (2015)  
Folyóiratcikk /Szakcikk /Tudományos
  5. *Haibin Wang, Xia Liu, Sheng Zhao, Lina Huo*  
Multi-authority E-voting System Based on Group Blind Signature  
**INTERNATIONAL JOURNAL OF ONLINE ENGINEERING** (ISSN: 1861-2121) 11: pp. 89-93. (2015)  
Folyóiratcikk /Szakcikk /Tudományos
  6. *Nihel Msilini, Lamri Laouamer, Bechir Alaya, Chaffa Hamrouni*  
Homomorphic Cryptosystems for Securing Data in Public Cloud Computing  
**INTELLIGENT SYSTEMS REFERENCE LIBRARY** (ISSN: 1868-4394) 115: pp. 59-75. (2017)  
Folyóiratcikk /Szakcikk /Tudományos
9. [Husztai A](#)  
Security Definitions for Electronic Exam Systems  
In: A Brodnik , G Galambos (szerk.)  
Proceedings of the 2010 Mini-Conference on Applied Theoretical Computer Science: MATCOS-10 . 130 p.  
Konferencia helye, ideje: Koper , Szlovénia , 2010.10.13 -2010.10.14. Koper: University of Primorska Press,  
2011. pp. 127-130.  
(ISBN:978-961-6832-10-6)  
  
Befoglaló mű link(ek): [Teljes dokumentum](#), [SZTE Publicatio](#)  
Könyvrészlet /Konferenciaközlemény /Tudományos
10. [Husztai A](#), Aszalós L  
Applying Spi-calculus for Password

In: Attila Egri-Nagy , Emőd Kovács , Gergely Kovásznai , Gábor Kusper , Tibor Tómacs (szerk.)  
Proceedings of the 8th International Conference on Applied Informatics : January 27-30, 2010, Eger, Hungary .  
456 p.  
Konferencia helye, ideje: Eger , Magyarország , 2010.01.27 -2010.01.30. Eger: Eszterházy Károly College, 2011.  
pp. 295-302.  
2..  
(ISBN:978-963-9894-72-3)

Befoglaló mű link(ek): [OSZK](#), [WorldCat](#), [Egyéb URL](#)

Könyvrészlet /Konferenciaközlemény /Tudományos

Függő idéző: 1 Összesen: 1

1. \* *Aszalós L*  
A kommunikáció modális operátorai és azok alkalmazásai  
(2011.)  
*Habilitációs tézisek*  
Egyéb/Nem besorolt /Tudományos

11. Husztai A, Kovács Z  
Univerzális kriptográfiai protokoll e-felmérésekhez  
In: Cser L , Herdon M (szerk.)  
Informatika a felsőoktatásban 2011 konferencia . 1140 p.  
Konferencia helye, ideje: Debrecen , Magyarország , 2011.08.24 -2011.08.26. Debrecen: Debreceni Egyetem  
Informatikai Kar, 2011. pp. 592-600.  
(ISBN:978-963-473-461-1)

Befoglaló mű link(ek): [Teljes dokumentum](#)  
Könyvrészlet /Konferenciaközlemény /Tudományos

2010

12. Husztai A, Pethő A  
A secure electronic exam system  
**PUBLICACIONES MATHEMATICAE DEBRECEN 77:(3-4) pp. 299-312. (2010)**

*Folyóirat szakterülete: Mathematics (miscellaneous) helyzete: Q2*

Link(ek): [Zentralblatt für Mathematik](#), [Mathematical Reviews](#), [WoS](#)

Folyóiratcikk /Szakcikk /Tudományos

Független idéző: 27 Összesen: 27

1. *Al-Suhimat Fadi M S*  
The Effectiveness of Adopting Computer-Based Examination in UUM  
(2010.)  
Egyéb /Diplomamunka, szakdolgozat, TDK dolgozat
2. *Meng Z, Lu J*  
Implementing the Emerging Mobile Technologies in Facilitating Mobile Exam System  
In: 2nd International Conference on Networking and Information Technology. Hong Kong: IACSIT Press, 2011. (ISBN 978-981-07-0680-7) pp. 80-88.  
Könyvrészlet /Konferenciaközlemény /Tudományos
3. *A Pavic, F Skopljanac-Macina*  
Computer in testing the Fundamentals of electrical engineering at the University of Zagreb Faculty of electrical engineering and computing  
In: Petar Biljanovic (szerk.) : Proceedings of the 35th International Convention MIPRO. 2012. (ISBN 978-1-4673-2577-6) pp. 1205-1210.  
Könyvrészlet /Konferenciaközlemény /Tudományos
4. *G Meletiou, I Voyiatzis, V Stavroulaki, C Sgouroupoulou*  
Design and Implementation of an E-exam System Based on the Android Platform  
In: 16th Panhellenic Conference on Informatics. Piraeus, Görögország: 2012.10.05-2012.10.07. (2012.) , pp. 375-380 .  
Egyéb konferenciaközlemény /Konferenciaközlemény /Tudományos
5. *Ribarski P, Antovski L*  
Mixnets: implementation and performance evaluation of decryption and re-encryption types  
In: LuzarStiffler V, Jarec I, Bekic Z (szerk.) : Proceedings of the ITI 2012 34th International Conference on Information Technology Interfaces. New York: Institute of Electrical & Electronics Engineers (IEEE), 2012. (ISBN 978-953-7138-24-0) pp. 493-498.  
Könyvrészlet /Konferenciaközlemény /Tudományos
6. *G Kambourakis*  
Security and Privacy in m-Learning and Beyond: Challenges and State-of-the-art  
**INTERNATIONAL JOURNAL OF U AND E SERVICE, SCIENCE AND TECHNOLOGY** (ISSN: 2005-4246) 6: (3) pp. 67-84. (2013)  
Folyóiratcikk /Szakcikk /Tudományos
7. *Buchmann J, Demirel D, van de Graaf J*  
Towards a Publicly-Verifiable Mix-Net Providing Everlasting Privacy  
In: Sadeghi A R (szerk.) : Financial Cryptography and Data Security. (7859) Berlin; Heidelberg: Springer Verlag, 2013. (ISBN 978-3-642-39883-4) pp. 197-204.  
(Lecture Notes in Computer Science)  
Link(ek): [DOI](#)  
17th International Conference, FC 2013, Okinawa, Japan, April 1-5. 2013.  
Könyvrészlet /Konferenciaközlemény /Tudományos

8. *R Giustolisi, G Lenzini, B Giampaolo*  
What security for electronic exams?  
In: 8th International Conference on Risk and Security of Internet and Systems (CRiSIS). La Rochelle, Franciaország: 2013.10.23-2013.10.25. (2013.), pp. 1-5.  
Paper 10.1109/CRiSIS.2013.6766348.  
Link(ek): [DOI](#)  
Egyéb konferenciaközlemény /Konferenciaközlemény /Tudományos
9. *Al-Saleem S M, Ullah H*  
A review of security considerations and palm based authentication scheme for computer based testing  
In: IEEE (szerk.): 9th International Conference on Computer Science & Education (ICCSE 2014). IEEE, 2014. (ISBN 978-1-4799-2952-8) pp. 291-293.  
Link(ek): [DOI](#)  
Könyvrészlet /Konferenciaközlemény /Tudományos
10. *Jannik Dreier, Rosario Giustolisi, Ali Kassem, Pascal Lafourcade, Gabriele Lenzini, Peter Y A Ryan*  
Formal Analysis of Electronic Exams  
In: Mohammad S Obaidat, Andreas Holzinger, Pierangela Samarati (szerk.): SECRYPT 2014 - Proceedings of the 11th International Conference on Security and Cryptography, Vienna, Austria, 28-30 August, 2014. Setúbal: SciTePress, 2014. (ISBN 978-989-758-045-1) pp. 101-112.  
Link(ek): [Teljes dokumentum](#)  
Könyvrészlet /Konferenciaközlemény /Tudományos
11. *J Dreier, R Giustolisi, A Kassem, P Lafourcade, G Lenzini*  
On the Verifiability of (Electronic) Exams  
Technical Report. (2014.)  
  
Link(ek): [Teljes dokumentum](#)  
Egyéb /Kutatási jelentés (közzétett) /Tudományos
12. *R Giustolisi, G Lenzini, P Ryan*  
Remark!: A Secure Protocol for Remote Exams  
In: Bruce Christianson, James Malcolm, Vashek Matyáš, Petr Švenda, Frank Stajano, Jonathan Anderson (szerk.): Security Protocols XXII. Springer, 2014. (ISBN 978-3-319-12399-8) pp. 38-48. (Lecture Notes in Computer Science)  
Link(ek): [DOI](#)  
Könyvrészlet /Konferenciaközlemény /Tudományos
13. *Bella G, Giustolisi R, Lenzini G*  
Secure exams despite malicious management  
In: Ali Miri (szerk.): Twelfth Annual Conference on Privacy, Security and Trust (PST 2014). Seattle: IEEE, 2014. 8 p. (ISBN 978-1-4799-3504-8) pp. 274-281.  
Link(ek): [DOI](#)  
Könyvrészlet /Konferenciaközlemény /Tudományos
14. *Saleh M Al-Saleem, Hanif Ullah*  
Security Considerations and Recommendations in Computer-Based Testing  
**SCIENTIFIC WORLD JOURNAL** (ISSN: 1537-744X) &: pp. 1-7. (2014)  
Link(ek): [DOI](#), [WoS](#)  
Folyóiratcikk /Szakcikk /Tudományos
15. *Demirel Denise*  
Universally Verifiable Poll-Site Voting Schemes Providing Everlasting Privacy  
2014.  
Disszertáció /PhD /Tudományos
16. *Jannik Dreier, Rosario Giustolisi, Ali Kassem, Pascal Lafourcade, Gabriele Lenzini*  
A Framework for Analyzing Verifiability in Traditional and Electronic Exams  
In: Information Security Practice and Experience. (9065) Springer, 2015. pp. 514-529. (Lecture Notes in Computer Science)  
Könyvrészlet /Konferenciaközlemény /Tudományos
17. *Dreier Jannik, Giustolisi Rosario, Kassem Ali, Lafourcade Pascal, Lenzini Gabriele*  
A Framework for Analyzing Verifiability in Traditional and Electronic Exams  
**LECTURE NOTES IN ARTIFICIAL INTELLIGENCE** (ISSN: 0302-9743) 9065: (Beijing) pp. 514-529. (2015)  
Link(ek): [DOI](#), [WoS](#)  
Folyóiratcikk /Tudományos
18. *Bella Giampaolo, Giustolisi Rosario, Lenzini Gabriele, Ryan Peter Y A*  
A Secure Exam Protocol Without Trusted Parties  
**IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY** (ISSN: 1868-4238) 455: (Hamburg) pp. 495-509. (2015)  
Link(ek): [DOI](#), [WoS](#)  
Folyóiratcikk /Tudományos
19. *S Dimitriou*  
Building an online examination system  
In: Proceedings of 2nd Hellenic Open Business Administration International Conference. HOBA, 2015. pp. 1-8.  
Könyvrészlet /Konferenciaközlemény /Tudományos
20. *LT Olçüoğlu, S Akleylek*  
Data Storage of Electronic Exams  
In: Proceedings of 8th International Conference on Information Security and Cryptology. Semor, 2015. pp. 1-5.  
Könyvrészlet /Konferenciaközlemény /Tudományos
21. *Rosario Giustolisi*  
Design and Analysis of Secure Exam Protocols  
2015.  
Disszertáció /PhD /Tudományos
22. *Jannik Dreier, Rosario Giustolisi, Ali Kassem, Pascal Lafourcade, Gabriele Lenzini, Peter Y A Ryan*  
Formal Security Analysis of Traditional and Electronic Exams  
In: E-Business and Telecommunications. (554) Springer, 2015. pp. 294-318. (Communications in Computer and Information Science)  
Könyvrészlet /Konferenciaközlemény /Tudományos
23. *Dreier Jannik, Giustolisi Rosario, Kassem Ali, Lafourcade Pascal, Lenzini Gabriele, Ryan Peter Y A*  
Formal Security Analysis of Traditional and Electronic Exams  
**COMMUNICATIONS IN COMPUTER AND INFORMATION SCIENCE** (ISSN: 1865-0929) 554: (Vienna) pp. 294-318. (2015)  
Link(ek): [DOI](#), [WoS](#)  
Folyóiratcikk /Konferenciaközlemény /Tudományos
24. *Nazmul Islam, Jahanara Pervin*  
Pragmatic Analysis of An Anonymous Network  
Lambert Academic Publishing, 2015.

Könyv /Szakkönyv /Tudományos

- 25 *Kissan Gauns Dessai, Venkatesh Kamat*  
A Framework for Analyzing Associativity and Anonymity in Conventional and Electronic Summative Examinations  
**LECTURE NOTES IN COMPUTER SCIENCE** (ISSN: 0302-9743) 10063: pp. 303-323. (2016)  
Folyóiratcikk /Konferenciaközlemény /Tudományos
- 26 *Farzin Shervin, Dahlan Halina Mohamed*  
PROPOSING A MODEL TO PREDICT STUDENTS' PERCEPTION TOWARDS ADOPTING AN E-ASSESSMENT SYSTEM  
**JOURNAL OF THEORETICAL AND APPLIED INFORMATION TECHNOLOGY** (ISSN: 1992-8645) 90: (1) pp. 144-153. (2016)  
Folyóiratcikk /Szakcikk /Tudományos
- 27 *Giampaolo Bella, Rosario Giustolisi, Gabriele Lenzi, Peter Y A Ryan*  
Trustworthy exams without trusted parties  
**COMPUTERS & SECURITY** (ISSN: 0167-4048) In Press: p. -. (2016)  
Folyóiratcikk /Szakcikk /Tudományos

2008

13. Husztai A  
Generalized Number Systems and Secure Electronic Elections  
Témavezető(k): Pethő A.  
2008.  
Disszertáció /PhD /Tudományos

14. Husztai A, Pethő A  
A Secure Electronic Exam System  
In: Pethő Attila , Herdon Miklós (szerk.)  
Informatika a felsőoktatásban 2008: Előadás-összefoglalók és teljes előadást tartalmazó CD-melléklet . 227 p.  
Konferencia helye, ideje: Debrecen , Magyarország , 2008.08.27 -2008.08.29. Debrecen: Debreceni Egyetem  
Informatikai Kar, 2008. pp. 1-7.  
(ISBN:978-963-473-129-0)

Befoglaló mű link(ek): [Teljes dokumentum](#), [Egyéb URL](#)

Könyvrészlet /Konferenciaközlemény /Tudományos

Független idéző: 8 Összesen: 8

1. *O Adebayo, S M Abdulhamid*  
E- Exams System for Nigerian Universities with Emphasis on Security and Result Integrity  
In: The Seventh International Conference on eLearning for Knowledge-Based Society. Bangkok, Thaiföld: 2010.12.16-2010.12.17. (2010.) , pp. 1-11 .  
Egyéb konferenciaközlemény /Konferenciaközlemény /Tudományos
2. *M V Adegbiya, M A Fakomogbon, F O Daramola*  
The New Technologies and the Conduct Of E-Examinations: A Case Study of National Open University of Nigeria  
**British Journal of Science** 3: (1) pp. 59-66. (2012)  
Link(ek): [Teljes dokumentum](#)  
Folyóiratcikk /Szakcikk /Tudományos
3. *Fagbola Temitayo M, Adigun Adebisi A, Oke Alice O*  
Computer- Based Test (Cbt) System For University Academic Enterprise Examination  
**INTERNATIONAL JOURNAL OF SCIENTIFIC AND TECHNOLOGY RESEARCH** (ISSN: 2277-8616) 2: (8) pp. 336-342. (2013)  
Link(ek): [Teljes dokumentum](#)  
Folyóiratcikk
4. *Fayyumi A, Zarrad A*  
Novel Solution Based on Face Recognition to Address Identity Theft and Cheating in Online Examination Systems  
**ADVANCES IN INTERNET OF THINGS** (ISSN: 2161-6817) 4: pp. 5-12. (2014)  
Link(ek): [DOI](#)  
Folyóiratcikk /Szakcikk /Tudományos
5. *SK Nayak, KM Alaskar*  
Hybrid Recommender System for Assessment in Multi-Constraint Academic Paradigm: A Review  
**INTERNATIONAL JOURNAL OF EMERGING TRENDS AND TECHNOLOGY IN COMPUTER SCIENCE** (ISSN: 2278-6856)  
4: (5/2) pp. 23-27. (2015)  
Folyóiratcikk /Szakcikk /Tudományos
6. *Ayham Fayyumi, Khaled Suwais*  
Online Exam Questions Distribution Technique based on Terminals Locations: The Case of Arab Open University  
**Journal of Computations & Modelling** (ISSN: 1792-7625) 5: (1) pp. 13-25. (2015)  
Folyóiratcikk /Szakcikk /Tudományos
7. *Emmanuel Okokondem Okon, Joshua B Agbogun*  
Software Quality and Usability for Computer-Based Test in Tertiary Institution in Nigeria: A Case Study of Kogi State University  
**AMERICAN JOURNAL OF EDUCATIONAL RESEARCH** (ISSN: 2327-6126) 3: (10) pp. 1224-1229. (2015)  
Folyóiratcikk /Szakcikk /Tudományos
8. *A Alnawaiseh, S Alnawaiseh*  
The attitude of information technology students in Mutah University towards computerized exams  
**EUROPEAN SCIENTIFIC JOURNAL** (ISSN: 1857-7881) 11: (34) pp. 416-428. (2015)  
Folyóiratcikk /Szakcikk /Tudományos

2007

15. Folláth J , Husztai A , Pethő A  
DESIGN In Asymmetric Authentication System

In: Emőd Kovács , Péter Olajos , Tibor Tómacs (szerk.)

Proceedings of the 7th International Conference on Applied Informatics . 792 p.

Konferencia helye, ideje: Eger , Magyarország , 2007.01.28 -2007.01.31. Eger: BVB Nyomda és Kiadó Kft., pp. 53-61. 1-2

Link(ek): [Zentralblatt für Mathematik](#)

Befoglaló mű link(ek): [Teljes dokumentum](#)

Egyéb konferenciaközlemény /Konferenciaközlemény /Tudományos

Független idéző: 1 Fügő idéző: 1 Összesen: 2

1. *Takács Péter*  
Kriptográfiai protokollok formális vizsgálata a CSN logikai rendszer bővítésével  
2009.  
Link(ek): [DEA](#)  
Disszertáció /PhD /Tudományos
2. \* *Folláth János*  
Kriptográfiai hash függvények és álvéletlenség generátorok  
2012.  
Link(ek): [DEA](#)  
Disszertáció /PhD /Tudományos

16. [Huszi A](#), Scheicher K , Surer P , Thuswaldner J M

Three-dimensional symmetric shift radix systems

**ACTA ARITHMETICA** 129: pp. 147-166. (2007)

*Folyóirat szakterülete: Algebra and Number Theory helyzete: Q3*

Folyóiratcikk /Szakcikk /Tudományos

Független idéző: 1 Fügő idéző: 7 Összesen: 8

- 1 \* *Barat G, Berthe V, Liardet P, Thuswaldner J*  
Dynamical directions in numeration (Dynamique de la numeration)  
**ANNALES DE L'INSTITUT FOURIER** (ISSN: 0373-0956) 56: (7) pp. 1987-2092. (2006)  
Folyóiratcikk /Szakcikk /Tudományos
- 2 \* *Surer P*  
 $\epsilon$ -shift radix systems and radix representations with shifted digit sets  
**PUBLICATIONES MATHEMATICAE DEBRECEN** (ISSN: 0033-3883) 74: (1.-2.) pp. 19-43. (2009)  
Folyóiratcikk /Szakcikk /Tudományos
- 3 \* *Kirschenhofer P, Pethő A, Surer P, Thuswaldner J*  
Finite and periodic orbits of shift radix systems  
**JOURNAL DE THEORIE DES NOMBRES DE BORDEAUX** (ISSN: 1246-7405) 22: pp. 421-448. (2010)  
Folyóiratcikk /Szakcikk /Tudományos
- 4 \* *Brunotte H, Kirschenhofer P, Thuswaldner J*  
Contractivity of three-dimensional shift radix systems with finiteness property  
**JOURNAL OF DIFFERENCE EQUATIONS AND APPLICATIONS** (ISSN: 1023-6198) &: Paper &. (2011)  
Folyóiratcikk /Szakcikk /Tudományos
5. \* *P Kirschenhofer, J Thuswaldner*  
Shift radix systems - A survey  
(2013.)  
  
Egyéb
- 6 \* *Klaus Scheicher, Victor F Sirvent*  
Automatic  $\beta$ -expansions of formal Laurent series over finite fields  
**FINITE FIELDS AND THEIR APPLICATIONS** (ISSN: 1071-5797) 27: pp. 1-23. (2014)  
Folyóiratcikk /Szakcikk /Tudományos
7. \* *K Scheicher, VF Sirvent, P Surer*  
Beta-expansions of p-adic numbers  
Arxiv preprint. (2014.)  
  
Egyéb /Folyóirat vagy sorozatszerkesztés /Tudományos
- 8 *Clemens Fuchs, Lajos Hajdu*  
30 years of collaboration  
**PERIODICA MATHEMATICA HUNGARICA** (ISSN: 0031-5303) pp. 1-20. (2016)  
Folyóiratcikk /Szakcikk /Tudományos

17. [Huszi A](#)

A Secure Electronic Voting Scheme,

**PERIODICA POLYTECHNICA-ELECTRICAL ENGINEERING** 51:(3-4) pp. 141-146. (2007)

*Folyóirat szakterülete: Electrical and Electronic Engineering helyzete: Q4*

Folyóiratcikk /Szakcikk /Tudományos

Független idéző: 5 Összesen: 5

1. *Ben Adida*  
Helios: Web-based Open-Audit Voting  
In: The 17th USENIX Security Symposium. (2008.) , pp. 335-348.  
Egyéb konferenciaközlemény /Konferenciaközlemény /Tudományos
2. *Takács Péter*  
Kriptográfiai protokollok formális vizsgálata a CSN logikai rendszer bővítésével  
2009.  
Disszertáció /PhD /Tudományos

- 3 *Eliver Pérez Villegas, Gina Gallegos-García, Gualberto Aguilar Torres, Héctor Flores Gutiérrez*  
Implementation of Electronic Voting System in Mobile Phones with Android Operating System  
***Journal of Emerging Trends in Computing and Information Sciences*** 4: (9) pp. 728-737. (2013)  
Folyóiratcikk
- 4 *Ayub Hussain Mondal, Manish Ranjan, Monjul Saikia*  
A Brief Overview of Homomorphic Cryptosystem and Their Applications  
***INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS*** (ISSN: 0975-8887) (2015)  
Folyóiratcikk /Szakcikk /Tudományos
5. *Eng Ahmed Abu Aziz*  
Using homomorphic cryptographic solutions on E-voting Systems  
(2015.)  
  
Egyéb /Diplomamunka, szakdolgozat, TDK dolgozat /Tudományos

2006

18. Pethő A , Brunotte H , Huszti A

Bases of canonical number systems in quartic algebraic number fields

***JOURNAL DE THEORIE DES NOMBRES DE BORDEAUX*** 18: pp. 537-557. (2006)

Link(ek): [Zentralblatt für Mathematik](#), [Mathematical Reviews](#), [DOI](#), [Egyéb URL](#)

Folyóiratcikk /Szakcikk /Tudományos

Független idéző: 9 Függő idéző: 3 Összesen: 12

- 1 \* *Akiyama S Brunotte H Pethő A*  
Reducible cubic CNS polynomials  
***PERIODICA MATHEMATICA HUNGARICA*** (ISSN: 0031-5303) 55: (2) pp. 177-183. (2007)  
Folyóiratcikk /Szakcikk /Tudományos
- 2 \* *Brunotte H*  
On Garcia numbers  
***ACTA MATHEMATICA ACADEMIAE PAEDAGOGICAE NYÍREGYHÁZIENSIS*** (ISSN: 0866-0182) 25: (1) pp. 9-16. (2009)  
Folyóiratcikk /Szakcikk /Tudományos
- 3 *Madritsch M G*  
Asymptotic normality of b-additive functions on polynomial sequences in number systems  
***RAMANUJAN JOURNAL*** (ISSN: 1382-4090) 21: (2) pp. 181-210. (2010)  
Folyóiratcikk /Szakcikk /Tudományos
- 4 *Ch Frougny, J Sakarovitch*  
Number representation and finite automata: Canonical numeration systems  
In: Berthé V, Rigo M (szerk.) : Combinatorics, Automata and Number Theory. (135) Cambridge: Cambridge University Press, 2010. 615 p. (ISBN 9780521515979) pp. 34-107. (Encyclopedia of Mathematics and its Applications)  
Könyvrészlet /Szaktanulmány /Tudományos
- 5 \* *Madritsch M G, Pethő A*  
Asymptotic normality of additive functions on polynomial sequences in canonical number systems  
***JOURNAL OF NUMBER THEORY*** (ISSN: 0022-314X) 131: (9) pp. 1553-1574. (2011)  
Folyóiratcikk /Szakcikk /Tudományos
- 6 *A Hameed, T Nakahara, SM Husnine*  
On existence of canonical number system in certain classes of pure algebraic number  
***JOURNAL OF PRIME RESEARCH IN MATHEMATICS*** (ISSN: 1817-2725) 7: pp. 19-24. (2011)  
Folyóiratcikk /Szakcikk /Tudományos
- 7 *Shigeki Akiyama, Paulius Drungilas, Jonas Jankauskas*  
Height reducing problems on algebraic integers  
***FUNCTIONES ET APPROXIMATIO COMMENTARII MATHEMATICI*** (ISSN: 0208-6573) 47: (1) pp. 105-119. (2012)  
Link(ek): [DOI](#), [Mathematical Reviews](#)  
Folyóiratcikk /Szakcikk /Tudományos
8. *J Jankauskas*  
Heights of Polynomials  
2012.  
Disszertáció /PhD /Tudományos
- 9 *P Drungilas*  
On a problem related to number system  
***SIAULIAI MATHEMATICAL SEMINAR*** (ISSN: 1822-511X) 7: (15) pp. 13-18. (2012)  
Link(ek): [Mathematical Reviews](#)  
Folyóiratcikk /Szakcikk /Tudományos
- 10 *Bérczes A, Evertse J-H, Györy K*  
Multiply monogenic orders  
***ANNALI DELLA SCUOLA NORMALE SUPERIORE DI PISA-CLASSE DI SCIENZE*** (ISSN: 0391-173X) 12: pp. 467-497. (2013)  
Link(ek): [Mathematical Reviews](#)  
Folyóiratcikk /Szakcikk /Tudományos
- 11 *Shahzad Ahmad, Toru Nakahara, Syed Muhammad Husnine*  
Power integral bases for certain pure sextic fields Read More:  
<http://www.worldscientific.com/doi/abs/10.1142/S1793042114500778?af=R>  
***INTERNATIONAL JOURNAL OF NUMBER THEORY*** (ISSN: 1793-0421) 10: (8) pp. 2257-2266. (2014)  
Link(ek): [DOI](#), [Mathematical Reviews](#)  
Folyóiratcikk /Szakcikk /Tudományos
- 12 *JH Evertse K Gyory*  
Discriminant Equations in Diophantine Number Theory  
Cambridge University Press, 2016.  
Könyv /Szakkönyv /Tudományos